In the Claims:

Please cancel claims 7-10. Please amend claims 1-5. Please add new claims 11-19. The claims are as follows.

a'

1. (Currently amended) A method for enabling ~~the~~ use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when ~~the~~ a private key and public key of a ~~any of the~~ certifying ~~authorities have~~ authority of the server has expired, comprising:

~~obtaining a server certifying authority chain (SCAC) certificate by the server from the said certifying authority;~~

~~presenting the~~ receiving an original ~~valid~~ authentication certificate ~~along~~ together with ~~the said~~ a server certifying authority chain (SCAC) certificate by the ~~server to the~~ browser from the server during ~~the~~ a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority[[,]];

~~accepting the transaction by the browser after verification of~~ verifying by the browser the original authentication certificate using the expired public key of the certifying authority[[,]]; and

verifying by the browser the ~~said~~ SCAC certificate using ~~the~~ a new public key of the ~~said~~ certifying authority.

2. (Currently amended) [[A]] The method ~~as claimed in~~ of claim 1, wherein the ~~said server~~

~~certifying authority chain (~~SCAC[[)]] certificate is obtained by ~~each~~ the server whenever the certifying authority invalidates its public key, wherein the certificate is obtained by:

contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate[[,]];

verifying the request by the certifying authority using the server's public key[[,]]; and

a1

generating the SCAC certificate by the certifying authority using it's a new private key of the certifying authority and forwarding the SCAC certificate to the ~~said~~ server.

3. (Currently amended) [[A]] The method ~~as claimed in~~ of claim 2 wherein ~~the~~ generating ~~of~~ the ~~said~~ SCAC certificate includes ~~the authentication of~~ authenticating the server name, ~~and~~ the server public key, old certifying authority public key, and certifying authority name.

4. (Currently amended) [[A]] The method ~~as claimed in~~ of claim 1, ~~wherein~~ further comprising issuing by the certifying authority ~~in case of client will also issue~~ a client ~~certificates known as~~ (CCAC) certificate[[s]], ~~which will work the same way as (SCAC) certificates~~ said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

5. (Currently amended) [[A]] The method ~~as claimed in~~ of claim 1, wherein ~~during SSL handshake when~~ the ~~client presents its certificate, it will also~~ method further comprises

presenting the CCAC certificate to the server during the handshake.

6. (Original) In an arrangement of networked server and browser systems conducting secure transactions and including a certifying authority for authenticating such transactions, characterized in that it includes a means for authenticating transactions when the public and private key of the said certifying authority have expired but the authentication certificates of any of server or browser systems is still valid, comprising:

a means for the server to obtain a certifying authority chain certificate using the new private key of the certifying authority,

a means for presenting the said certifying authority chain certificate together with the original authentication certificate, to the browser,,

a means for verifying the original authentication certificate using the expired public key of the certifying authority, and verifying the certifying authority chain certificate using the new certifying authority public key by the browser.

7. (Canceled)

8. (Canceled)

9. (Canceled)

10. (Canceled)

11. (New) The method of claim 1, further comprising accepting the transaction by the browser after said verifying the original authentication certificate and after said verifying the SCAC certificate.

12. (New) The method of claim 1, wherein obtaining the SCAC certificate comprises using the new private key of the certifying authority.

a1

13. (New) A system for enabling use by a browser of valid authentication certificates in relation to a transaction between the browser and a server when a private key and public key of a certifying authority of the server has expired, comprising:

means for receiving an original authentication certificate together with a server certifying authority chain (SCAC) certificate by the browser from the server during a SSL handshake between the browser and the server, said SCAC certificate having been previously obtained by the server from the certifying authority;

means for verifying by the browser the original authentication certificate using the expired public key of the certifying authority; and

means for verifying by the browser the SCAC certificate using a new public key of the certifying authority.

14. (New) The system of claim 13, wherein the SCAC certificate is obtained by the server whenever the certifying authority invalidates its public key, wherein the certificate is

obtained by:

means for contacting the certifying authority using the server's private key for authentication to make a request for the SCAC certificate;

means for verifying the request by the certifying authority using the server's public key; and

means for generating the SCAC certificate by the certifying authority using it's a new private key of the certifying authority and forwarding the SCAC certificate to the server.

a1

15. (New) The system of claim 13, wherein said means for generating the SCAC certificate includes means for authenticating the server name, the server public key, old certifying authority public key, and certifying authority name.

16. (New) The system of claim 15, further comprising means for issuing by the certifying authority a client(CCAC) certificate, said CCAC certificate being functionally the same as the SCAC certificate subject to the roles of the browser and the server being interchanged.

17. (New) The system of claim 13, wherein the system further comprises means for presenting the CCAC certificate to the server during the handshake.

18. (New) The system of claim 13, further comprising means for accepting the transaction by

a1

the browser in conjunction with said means for verifying the original authentication certificate and in conjunction with said means for verifying the SCAC certificate.

19. (New) The system of claim 13, wherein said means for obtaining the SCAC certificate comprises use of the new private key of the certifying authority.